Exhibit F

RANDALL S. LUSKEY (SBN: 240915)
rluskey@paulweiss.com
**PAUL, WEISS, RIFKIND, WHARTON
& GARRISON LLP**
535 Mission Street, 24th Floor
San Francisco, CA 94105
Telephone: (628) 432-5100
Facsimile: (628) 232-3101

ROBERT ATKINS (*Pro Hac Vice* admitted)
ratkins@paulweiss.com
CAITLIN E. GRUSAUSKAS (*Pro Hac Vice* admitted)
cgrusauskas@paulweiss.com
ANDREA M. KELLER (*Pro Hac Vice* admitted)
akeller@paulweiss.com
**PAUL, WEISS, RIFKIND, WHARTON
& GARRISON LLP**
1285 Avenue of the Americas
New York, NY 10019
Telephone: (212) 373-3000
Facsimile: (212) 757-3990

Attorneys for Defendants
UBER TECHNOLOGIES, INC.,
RASIER, LLC, and RASIER-CA, LLC

[Additional Counsel Listed on Following Page]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE: UBER TECHNOLOGIES, INC., PASSENGER SEXUAL ASSAULT LITIGATION

This Document Relates to:

ALL ACTIONS

Case No. 3:23-md-03084-CRB

DECLARATION OF JAMIE BROWN IN SUPPORT OF DEFENDANTS UBER TECHNOLOGIES, INC., RASIER, LLC, AND RASIER-CA, LLC'S PROPOSED ESI PROTOCOL

Judge: Hon. Lisa J. Cisneros
Courtroom: G – 15th Floor

MICHAEL B. SHORTNACY (SBN: 277035)
mshortnacy@shb.com
SHOOK, HARDY & BACON, L.L.P.
2049 Century Park East, Suite 3000
Los Angeles, CA 90067
Telephone: (424) 285-8330
Facsimile: (424) 204-9093

PATRICK OOT (*Pro Hac Vice* admitted)
oot@shb.com
SHOOK, HARDY & BACON, L.L.P.
1800 K Street NW, Suite 1000
Washington, DC 20006
Telephone: (202) 783-8400
Facsimile: (202) 783-4211

KYLE N. SMITH (*Pro Hac Vice* admitted)
ksmith@paulweiss.com
JESSICA E. PHILLIPS (*Pro Hac Vice* admitted)
jphillips@paulweiss.com
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
2001 K Street, NW
Washington DC, 20006
Telephone: (202) 223-7300
Facsimile: (202) 223-7420

Attorneys for Defendants
UBER TECHNOLOGIES, INC.,
RASIER, LLC, and RASIER-CA, LLC

I, Jamie Brown, declare under penalty of perjury as follows:

1. I am a Vice President of Global Advisory Services at Lighthouse. I am an attorney and legal consultant, specializing in information law, which includes e-discovery. I have over 23 years of in-house, government, and law firm experience, which I draw upon to advise clients on various challenges related to the use of information and technology in the context of litigation and investigations. My prior experience includes working for UBS, where, as Executive Director and Global eDiscovery Counsel, I was responsible for designing, implementing, and managing the company's global e-discovery programs to support the firm's global litigation and investigation docket. I also worked for Barclays, leading and implementing a global program to reduce legal, regulatory, and privacy risk associated with legacy systems and data. Prior to my years in corporate practice, I spent several years in government service, first as a trial attorney in the Division of Enforcement at the U.S. Commodity Futures Trading Commission in Washington, D.C., and later, as Assistant General Counsel, Head of eDiscovery and Information Governance, where I served as the Agency's resident e-discovery expert. My career began as a litigation associate at King & Spalding LLP, and later, as a partner at Fennemore Craig specializing in information law. Through the aforementioned roles, I have managed eDiscovery for hundreds of complex litigation matters (from inception through conclusion) and consulted with hundreds of clients on various challenges associated with information and technology, particularly as it evolves.

2. I submit this declaration at Uber Technologies, Inc.'s ("Uber") and its outside counsel, Paul Weiss and Shook Hardy Bacon's request, and in support of Uber's Proposed ESI Protocol. I understand a dispute has arisen involving Uber's ability to collect and produce certain documents shared by email and chat via reference links. I am familiar with the facts contained herein and am prepared to testify to the extent required.

3. In preparing this declaration, I undertook the following steps: (1) I conducted internal interviews with Lighthouse team members who have firsthand knowledge and experience with Uber and the facts and circumstances set forth below; (2) I interviewed William Anderson from Uber to confirm Lighthouse's understanding of Uber's internal eDiscovery processes and use of Google

Workspace and Google Vault's technology; (3) I interviewed Arman Gungor from Metaspike to confirm Lighthouse's understanding of Metaspike's Forensic Email Collector's ("FEC") capabilities; (4) I reviewed Pretrial Order No. 9: Order on ESI Protocol Disputes, ECF No. 345 in the above-captioned action; and I reviewed "Plaintiffs Proposed Methodology for Retrieving Google Drive Documents Linked to Within Google Emails."

Google Workspace

4. Uber uses Google Workspace (Business and Enterprise Edition), which offers a suite of web-based applications, including but not limited to **Gmail** (for email), **Google Chat** (for chat messaging), and **Google Drive** (for file storage and collaboration). Uber's edition of Google Workspace also includes a tool called **Google Vault** ("Vault") that supports information governance and eDiscovery, including but not limited to the retention, preservation, collection, search and export of Google data.

5. Lighthouse provides eDiscovery services to Uber, and has worked with Uber since 2019.[1] Since that time, Uber has been using Google Workspace, formerly known as G-Suite. Uber has also used Vault for, in relevant part, enabling retention, deletion and legal hold policies against Google data (*i.e.*, documents and information stored or communicated via a Google product described above).

6. It is my understanding that, in connection with this MDL, Uber's eDiscovery Team has collected (and is continuing to collect) relevant Gmail, Google Chat and Google Drive data using Vault, which it provided (and continues to provide) to Lighthouse for processing, hosting and review by its outside counsel.

Background on Shared Documents / Linked Drive Files

7. To provide some background, traditionally, documents have been shared by email or chat in one of two ways: by uploading a copy of a file as a physical attachment or by embedding the file into the message. In both scenarios, the file was static (meaning, it was not subject to being modified by another user in the normal course of business), and metadata naturally existed that would

[1] Uber began working with a company called H5, which Lighthouse acquired on August 11, 2021.

allow for the ready association of that document to the message by an eDiscovery vendor. Over time, this ready association paved the way for an industry standard of producing the attachment with the underlying message based on the notion that it was part of a "parent-child" relationship (where the message is the parent, and the child is the attachment).

8. Cloud based technologies provide a very different file sharing mechanism that embeds a link within the body of the message that points to a document's storage location. The underlying document is not static, but rather, dynamic – it can be edited, moved, or deleted, depending on how the system is configured, who has access to the document, and how it is used over the course of time. Some systems allow for file sharing only via reference links, while others allow the option of providing a traditional attachment.[2]

9. Cloud based technologies also provide a different mechanism for creating versions of documents ("versioning") that is "system driven" as opposed to "user driven." System driven versioning refers to the automatic creation of a new version when changes are made to a document (based on system specifications); in practice, this can yield potentially hundreds of versions without any user intention or sometimes, even knowledge that a version is being created. In contrast, user driven versioning (which was commonplace with word processing applications until they were replaced by cloud-based systems) relies upon a user to intentionally create a new version.

10. Versioning is material to the discussion of shared documents because of how eDiscovery tools access and retrieve this information. Typically, there are two types of tools used to access and retrieve enterprise data: features that are built-in to a system "natively," such as those in

[2] These reference links are sometimes referred to as hyperlinks, although a hyperlink (by definition) is broader, as it also includes links to websites, web applications and data or document locations. The practice of hyperlinking dates back 20+ years and refers to the technical capability of moving from one data location to another for various purposes.
Reference links have also been referred to as cloud "attachments," which can be a misnomer to the extent the treatment of this method of file sharing is considered the same as with physical attachments (note that, some cloud technologies provide the option to send a traditional attachment, and nothing about the cloud technology changes how such an attachment should be considered in the context of eDiscovery).
Cloud providers adopt their own terminology to describe their file sharing technology, and Google uses the term "linked Drive files" (for reference, Microsoft uses the term "cloud attachment," and previously used the term "modern attachment").

Vault (for Google data) or Purview (for Microsoft data), or third-party collection tools that are used to access a company's systems for this purpose. In most cases, the built-in eDiscovery features used to collect data from enterprise systems cannot readily access and retrieve the precise version of the document shared ("version shared") when collecting communications, but rather, only the last version of the linked document, if at all.[3]

11. The same is true for Vault: if a Vault user seeks to collect and export shared documents (as part of a message collection), today, they can do so, but the only option is to include the last version of the linked Drive documents.[4]

12. Before December 2023, however, even this feature (of collecting shared documents as part of a message collection) did not exist within Vault. Rather, should a Vault user need to collect shared documents as part of a message collection, a Vault user would need to collect the Gmail or Google Chat first, then collect the individual custodian's Google Drive as two separate collection tasks and, even still, the collection would include only the last version. The company would then need to use a third-party tool or parser to associate the message with the shared document. The December 2023 feature change simplified the process of collecting shared documents (as part of a message collection), although nothing changed with respect to the fact that Vault only provided the option of collecting the last version.

[3] Microsoft Purview (Premium Version only, as opposed to the Standard Version) released new functionality in April of 2023 that collects the version shared as part of a message collection, but only if the company specifically enables this feature; there are other caveats, including that the company needs to use a Premium eDiscovery workflow to collect and export the data, which carries significant implications (something that is beyond the scope of this declaration given that Uber does not use this technology, but worth noting given the market confusion around how the different technology works and the myriad considerations required to deploy these enterprise tools in holistic manner to meets a company's legal, regulatory, security, privacy and business requirements, all of which takes time and careful consideration). Notably, the ability to collect and export version shared within Premium only applies prospectively, not retroactively – in other words, only to documents created from the point at which the feature was enabled in OneDrive or Sharepoint, and only for the locations within the scope of the policy.

[4] Vault also does not provide for the retention, preservation or search of versions shared *in the context of the communication*. Vault *does* allow versions to be retained, and thus, preserved (rendering them available for collection as a *separate* collection activity – one that is extremely manual and not part of a standard eDiscovery collection workflow), but there is no metadata available that would associate the version shared with the communication. –

13. As a result of technical differences in the way documents are created (including versioning), stored, shared and managed within newer cloud-based technologies like Google Workspace, and the options users have to perform eDiscovery tasks within these tools (*e.g.*, using Vault), some Lighthouse clients have argued against (successfully) the routine collection and production of shared or linked documents in discovery on the basis:

a. Shared or linked documents are not, in fact, attachments for the reasons above;

b. Given the lack of available metadata to readily associate the shared document (version shared or, in some cases, also last version) with the message, no natural association exists between the message and the shared document;

c. Any linkage between the message and the shared document would require significant time, cost and burden to facilitate at scale;

d. Even when metadata is available within the eDiscovery tool to link the last version with the message, that metadata alone does not establish an association, where the document may have been modified after the message was sent.

14. Clients have further argued (successfully) that they will produce the version shared only upon a showing of need due to the extremely manual and cumbersome process involved.

15. Where this is not possible (such as for a regulatory investigation), some clients have opted to produce the last version of the shared document in lieu of the version previously shared between users at a given time on the basis that, at least they have the option to collect and export the document using the built-in eDiscovery features (*e.g.*, Vault). Depending on when the message and shared documents were collected, and the technology that existed at the time for obtaining metadata that naturally associates the shared document with the message, the client would then need to use a parser (typically through an eDiscovery vendor like Lighthouse) to create the association using other metadata.

16. The practices set forth in paragraphs 13-15 have recently emerged as the new industry standard for the handling of shared or linked documents.

17. Note that the collection of shared documents within Vault is not perfect and is subject to document access limitations.

18. I understand that, for the past four years, Uber's practice was and is to collect and produce the last version of the linked document using Vault's native capabilities. I further understand that Uber adopted this practice because, in 2020, the new industry standard for linked documents described in paragraphs 13-15 had not yet emerged, and Uber was under pressure to continue to produce shared documents in litigations in a traditional manner, despite the technical challenges of doing so. To meet pressing needs on pending matters, Uber hired Lighthouse to develop a custom "parser" tool that would associate the shared document (*i.e.*, last version) with the message where, at the time, Vault did not provide this metadata with the export.

19. In producing the last version of shared documents, Uber went over and beyond what most parties do today when collecting and producing documents in litigation, particularly given what was available using Vault's built-in eDiscovery features that existed up until December 2023.

Lighthouse's Google Parser

20. In 2020, Lighthouse developed a custom parser to address Uber's needs to parse Google chat and email messages ("Google Parse"). The Google Parser is not a collection tool, rather, it is used to extract specific data from email and chat messages that have *already* been collected and organize it to facilitate search, review and production. Lighthouse has used this parser successfully on Uber's behalf in more than 20 litigations and other matters.

21. Most major eDiscovery vendors provide their own proprietary parsing software. In contrast with other eDiscovery tools (*e.g.*, Relativity, one of the most ubiquitous tools available to review and produce documents), there is no predominant parsing software application licensed and used by the majority of eDiscovery vendors.

22. Lighthouse's Google Parser is primarily used to: (a) identify links to shared documents stored in Google Drive that appear in the top-most portion of a message; and (b) identify certain metadata associated with the linked document (specifically, the Google Document ID). This information, as well as the underlying messages and Drive data, is loaded into a review tool

(Relativity). From there, Lighthouse runs a script to identify where the linked Google Document ID's are present and stores this information in a unique field that then allows the message and document to be grouped together for purposes of review and production. Note that this creates an association between the message and the shared document, where one previously did not exist given that the Vault export did not contain metadata to support this naturally.

23. The Lighthouse Google Parser is unique in a few ways.

a. It only looks for links that appear in the top portion of the message (if it identified links embedded in earlier portions of the email thread, there could be numerous linked documents shared by other email participants that may not be custodians in the matter; if the participant is a custodian, then in theory, the messages contained in the thread, and any links shared, would be collected by Vault so long as they are within the relevant timeframe).

b. If the same document was shared by more than one custodian or in more than one message, it will only store one copy of the shared document (although the metadata will show with which messages it is associated). Note that the parser only applies to shared documents stored in Google Drive and not other storage locations.

c. It only contains certain metadata fields deemed relevant to the search, review and production of the messages; in contrast, it does not contain every metadata field available. Metadata fields are determined based upon the nature of the data and needs of the client, which are informed by the matter, agreed upon protocol and industry standard.

24. Even with a parser designed to identify links and create an association between a message and the shared document, not all documents will be located. For example, in some cases, a sender may forward a message containing a link that appears lower in the email chain (where the Google Parser only identifies links near the top of the message for the reasons stated above).

<u>Metaspike FEC</u>

25. While Plaintiffs' current proposal does not suggest the use of a tool called Metaspike Forensic Email Collector ("FEC"), Plaintiffs' expert previously suggested that FEC might be a viable alternative to collect the versions shared (as opposed to last versions).

26. Lighthouse uses FEC to collect email and documents only in certain limited matters involving small data volumes and where the collection at issue is extremely targeted. Although FEC can be an effective tool when Vault is not an option (for example, collecting an individual's personal Gmail) or to collect a shared version in cases that warrant it, there are numerous limitations:

- FEC cannot access data via Vault; rather, it uses an API that connects directly to the individual Google applications (*e.g.*, Gmail, Drive), and therefore, can access only "active" data (*i.e.*, data that is available within an individual user's workspace). This is a subset of what is available within Vault, whose purpose is for information governance and eDiscovery.
- FEC does not allow for the collection of data across custodians; rather, one would need to collect custodian-by-custodian, which is impractical in a matter with a large number of custodians.
- FEC does not allow for a "group export" of data; rather, one would need to export data on a custodian-by-custodian basis, which is impractical in a large matter.
- FEC does not permit the de-duplication of data across custodians.
- Although FEC does permit the collection of the version shared in some instances, there are additional challenges, including artificially creating a link between a message and the shared document anytime the link appears in an email message thread. In this circumstance, FEC will collect the version of the document that existed at the time the email was sent (and each subsequent reply), even if the document was not shared in subsequent replies. This presents a risk that a factfinder could conclude that certain email recipients received a copy of the shared document when, in fact, they did not – a risk that is compounded when a collection involves numerous custodians and large volumes of data. It also contributes to the overcollection of data (and costs associated therewith).

- FEC shares the same limitations as Vault when it comes to certain shared documents that are inaccessible (*e.g.*, lack of credentials).

27. Given these limitations, Lighthouse uses FEC only in the limited circumstances described above. For these reasons, Lighthouse would not recommend using FEC for a matter like this one, where there is a large volume of data, as it would be workable. Further, Lighthouse would not recommend using FEC given that Uber has Vault, which it is using as its document repository for Gmail and Drive data.

28. I spoke with Arman Gungor of Metaspike to specifically confirm my understanding that FEC cannot access Vault, which he confirmed. Mr. Gungor also mentioned that Metaspike will soon be announcing additional features for its FEC tool, which he acknowledged will still not enable FEC to access Vault. Metaspike has not yet announced these additional features, let alone made them commercially available, as Mr. Gungor stated that Metaspike was still testing them. Nevertheless, I discussed the additional features with Mr. Gungor, and they will not address the limitations described above. As a result, I would not recommend FEC for Uber in this matter.

Custom Solution

29. Plaintiffs' proposal suggests that Uber be required to build a custom solution to access Google's API's, identify the version shared of the linked documents (as opposed to the last version) and collect these documents.

30. Lighthouse does not believe such a proposed solution is workable. First, Plaintiffs' proposed use of Google's APIs only allow access to the applications directly (e.g., Gmail, Drive). As with FEC, there are limitations of accessing the data in this manner, as the proposed solution would only access active data and not data stored in Vault. Second, there are challenges with executing scripts to collect and export data via these APIs, which are only designed for lightweight use. Based on Lighthouse's experience, using the APIs in the manner Plaintiffs propose will yield a high volume of failures (i.e., scripts that cannot execute the task for which they are designed, causing the collection process to stop) for various reasons, including but not limited to scalability issues, system limits, and the frequent updates by Google to the APIs and underlying applications. In short, these APIs are

simply not amenable to this kind of code at the scale required.

31. Lighthouse would also not recommend taking this course of action given that Vault is Google's information governance and eDiscovery tool, which means it serves as the document management system for Google data that is potentially relevant in this litigation; it also serves as Google's repository for legal hold data. Plaintiffs are essentially asking Uber to create a new solution that bypasses Uber's document management system and legal hold repository to access whatever user data remains active within Google Drive. This would constitute an extraordinary measure that is inconsistent with foundational principles of data lifecycle management, which contemplate that companies retain data to meet various requirements, preserve data under legal hold, and collect relevant data (as a subset of what is typically under legal hold, depending) from the system or systems where this data resides in the ordinary course of business. Uber has a tool (Vault) that was built to support these foundational principles, Vault is fit-for-purpose, it is used by countless companies for this precise purpose, and Uber is using it to its fullest capabilities. Plaintiffs are asking Uber to build additional functionality that exceeds what can be done today.

32. Moreover, *even if* such a solution were successful, it would only yield a subset of the shared documents Plaintiffs seek and would require substantial recollection of data. Most eDiscovery vendors do not provide this type of custom development service (at the level needed to support this development), as it requires professional programming expertise that is not routinely requested by clients as part of standard eDiscovery process.

I affirm under penalty of perjury of the laws of the State of New York that the foregoing statement is true and correct. Executed on April 12, 2024 in New York, New York.

Jamie Brown

Jamie Brown